

UNITED STATES DISTRICT COURT

for the
District of Utah

SEALED

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
CELLPHONE AND STORAGE DEVICE AS
DESCRIBED IN ATTACHMENT A

Case No. 2:23mj190-DAO

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE "ATTACHMENT A"

located in the _____ State and _____ District of _____ Utah _____, there is now concealed (identify the person or describe the property to be seized):

SEE "ATTACHMENT B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 2242(b)	Coercion and Enticement
18 U.S.C. 2252(a)(2), et al.	Distribution of Child Pornography
18 U.S.C. 2252(a)(4), et al.	Possession of or Accessing with Intent to View Child Pornography

The application is based on these facts:

SEE AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT, which is attached to this Application

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

JEFFREY M CHMIELEWSKI Digitally signed by JEFFREY M CHMIELEWSKI
Date: 2023.03.01 13:37:06 -07'00'

Applicant's signature

Jeffrey M. Chmielewski, Special Agent, HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Zoom video conference (specify reliable electronic means).

Date: 03/02/2023

City and state: Salt Lake City, UT



Daphne A. Oberg

Judge's signature

Daphne A. Oberg, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, Jeffrey M. Chmielewski, a Special Agent with Homeland Security Investigations (HSI), assigned to the HSI Salt Lake City, Utah office, being duly sworn under oath, do hereby depose and state as follows:

Introduction and Agent Background

1. I have been employed by HSI since May 2020. I am currently assigned to the child exploitation unit in the HSI Office in Salt Lake City, Utah. I am concurrently assigned to the Utah Internet Crimes Against Children (ICAC) Task Force, managed by the Utah Attorney General's Office, and the Child Exploitation Task Force (CETF), managed by the Salt Lake City FBI Office. Prior to being employed by HSI, I was a Colorado State Patrol Trooper for approximately six (6) years. My formal law enforcement training includes completing the 14-week Criminal Investigator Training Basic (CITP) training course and the 15-week HSI Special Agent Training program at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. I have received additional training from CETF, ICAC, and other sources related to Child Sexual Abuse Material (CSAM), to include child pornography (as defined in 18 U.S.C. § 2256), and exploitation investigations and specifically to online, undercover enticement investigations.

2. As a federal agent, I am authorized to investigate violations and execute warrants issued under the authority of the United States. I am charged with the investigation of criminal violations relating to child exploitation and CSAM, including violations pertaining to the illegal production, distribution, receipt, and possession of CSAM and pertaining to the online enticement of a minor in violation of 18 U.S.C. §§ 2242(b), 2251, 2252, and 2252A.

3. I have been involved in investigations involving federal criminal violations related to the distribution, receipt, and possession of CSAM, child enticement and exploitation, and cybercrime. I have reviewed numerous examples of CSAM. I have become familiar with ways that CSAM is shared, stored, distributed, and/or produced, including the use of various social media websites (Facebook, Instagram Twitter, Kik, Snapchat, Discord, etc.), messaging platforms and applications, electronic media storage, “cloud” based storage, and peer-to-peer (P2P) networks. I have also become familiar with jargon or slang terms that people involved in child exploitation use to discuss their activities. I have gathered evidence pursuant to search warrants and have participated in searches of premises, persons, and electronic devices. I have conversed in undercover, online conversations with, and upon arrest, have interviewed persons who possess, view, and distribute CSAM or who seek to commit physical sexual offenses against minors.

Purpose of the Affidavit

4. I submit this affidavit in support of an application to search a cellular telephone (the “SUBJECT CELLPHONE”) and an electronic storage device (“the SUBJECT STORAGE DEVICE” of **Kendrick Aristotle EASTES (“EASTES”)** further described in **Attachment A** hereto, for contraband and evidence, fruits, and instrumentalities of violations of Coercion and Enticement in violation of 18 U.S.C. § 2422(b), Distribution of Child Pornography in violation of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), and Possession of or Accessing with Intent to View Child Pornography in violation of 18 U.S.C. §§ 2252(a)(4) and 2252A(a)(5)(B) (the “Target Offenses”) as described in **Attachment B** hereto.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. The facts set

forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Brief Summary

6. As set forth in detail below, on February 16, 2023, EASTES initiated an online conversation with an HSI undercover agent (UCA). In the course of the conversation, EASTES expressed his desire and then his intention to sexually abuse and sodomize a fictitious seven-year-old boy (child). EASTES distributed three images of apparent CSAM to the UCA, and said he would bring his “porn stash,” sexual lubricant, anal sex abuse devices to use on the child, and candy for the child.

7. EASTES drove to the location of the child, and upon contact with agents and his arrest, had with him the SUBJECT CELLPHONE, SUBJECT STORAGE DEVICE with USB-C adapter which interfaces with the SUBJECT CELLPHONE, two bags of candy for the child, two types of sex lubricant, adult anal sex devices, and the purchase receipt for the lubricant and sex devices. The SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE were seized and booked in as evidence. As EASTES distributed apparent CSAM, stated he was bringing his (child) pornography collection, and arrived with electronic storage devices capable of storing CSAM, there is probable cause to believe that contraband and evidence, fruits, and instrumentalities of the Target Offenses, as described in **Attachment B**, will be located in the SUBJECT CELLPHONE and the SUBJECT STORAGE DEVICE as described in **Attachment A**.

Applicable Law

8. As noted above, this investigation concerns alleged violations of the following Target Offenses:

a. 18 U.S.C. § 2422(a) prohibits any person from, using the mail or any facility or means of interstate or foreign commerce to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempt to do so.

b. 18 U.S.C. § 2252(a)(2) prohibits any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. 18 U.S.C. § 2252(a)(4)(B) prohibits any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce

or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

d. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

e. 18 U.S.C. § 2252A(a)(5)(B) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

Background on Computers and CSAM (Child Pornography)

9. Based on my knowledge, training, and experience in child exploitation and CSAM investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers, computer technology, and the Internet have drastically changed how CSAM is produced and distributed.

10. Computers serve four basic functions in connection with CSAM: production, storage, communication, and distribution.

11. Child pornographers can upload images or video clips directly from a digital camera to a computer. Once uploaded, they can easily be edited, manipulated, copied, and distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer using a scanner. Once uploaded, they too can easily be edited, manipulated, copied, and distributed. A modem allows any computer to connect to another computer via a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

12. The computer's ability to store images in digital form makes it an ideal repository for CSAM. The size of the electronic storage media (commonly referred to as the hard drive or more recently, memory) used in home computers has grown tremendously in the last several years. This storage can store millions of images at very high resolution. Images and videos of CSAM can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like, many of which are small, highly portable, and easily concealed, including on someone's person or inside their vehicle.

13. The Internet affords collectors of CSAM several different venues for obtaining, viewing, and trading CSAM in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs such as Kik, bulletin board services, e-mail, "peer-to-peer" (P2P) file sharing programs such as LimeWire and eMule, and networks such as eDonkey, Gnutella, ARES, Tumblr, and BitTorrent. Collectors and distributors of CSAM sometimes also use online resources such as "cloud" storage services to store and retrieve CSAM. Such online services allow a user to set up an account with a remote computing service that provides e-mail

services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet and can access stored files using any device capable of connecting to the Internet. Evidence of such online storage of CSAM is often found on the user's computer.

14. An Internet Protocol (IP) address is a unique identifier that electronic devices such as computers, routers, fax machines, printers, and the like use to identify and communicate with each other over a network. An IP address can be thought of as a street address. Just as a street address identifies a particular building, an IP address identifies a particular Internet or network access device. When a user logs on to his/her Internet Service Provider (ISP), they are assigned an IP address for the purpose of communication over the network. An IP address can be statically assigned, meaning the IP address does not change from one Internet session to another, or dynamically assigned, meaning a user receives a different IP address each time the user accesses the Internet. An IP address can only be assigned to one user at a time, and ISPs keep records of who IP addresses are assigned to by date and time. Similarly, cell phone service providers also generally keep IP records that can identify what device (cell phone) utilized the IP address on a certain date and time.

15. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in the computer's web cache and Internet history

files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

16. I know, based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including persons who collect and trade in CSAM, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such persons maintain their collections of CSAM in safe, secure, and private locations, such as their residence or vehicle, and on computers and digital storage media under their direct control. Such persons often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period. In some cases, however, persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of CSAM indefinitely.

17. I also know from my training and experience that many people who download CSAM from the Internet, and those who collect CSAM, frequently save images and videos of CSAM on their computers and/or transfer copies to other computers and storage media, including cloud storage accounts, external hard drives, thumb drives, flash drives, SD cards, and CDs or DVDs. Moreover, it is common in child exploitation investigations to find CSAM on multiple devices and/or storage media located in suspects' homes, rather than on a single device.

18. I know based on my training and experience that many social media and messaging platforms, such as Facebook, Instagram, Twitter, Signal, Snapchat, Kik messenger,

and others can be directly accessed and used with one's cellular phone. Often, these applications require the user to download the application directly to their phone, which then allows seamless use between the cellular phone and the social media or messaging website.

Statement of Probable Cause

A. HSI Conducts Undercover, Online Chat with EASTES

19. On February 16, 2023, a Homeland Security Investigations (HSI) agent was acting in an undercover capacity on online cellphone social media, dating, and messaging applications (apps). On one such app, Application A¹, the undercover agent (UCA) was the recipient of messages from dozens of users within a period of a few hours. On this geo-locating app, the UCA used a profile name of "NLTabDad," a 27-year-old male with a "selfie" photo in a gym-setting showing shoulders to knees, wearing gray shorts and a black shirt pulled up to show his stomach and part of his chest. The term "Taboo," or "Tab" is often used on these apps to denote something that is forbidden on grounds of morality or taste, and "NL" is a reference to "no limits."

20. The UCA responded on Application A to several of the users who initiated a conversation with the UCA and continued a conversation with only two of those users. Application A user "Kisuke," who was later identified as EASTES, displayed as a 31-year-old male, online now, two miles away, with additional physical descriptors including height, weight, gender, and ethnicity.

¹ The name of Messaging Platform A is known to law enforcement and intentionally omitted to protect the ongoing investigation. The name of the social media platform will be provided upon the Court's request.

21. EASTES initiated contact on Application A with the UCA at approximately 2239 hours by stating “Lol, love that name”, referring the UCA’s username, “NLTabDad.” EASTES followed with “I mean the taboo stuff is the most fun”² and “Wish I had something smooth to wrap my meat in for that matter”. The UCA asked EASTES if he wanted to text message and provided his phone number, and EASTES agreed, but stated he wanted to use Signal, an end-to-end encrypted messaging app. EASTES confirmed in Application A that he had texted the UCA, who had received a text message from phone number 505-333-XXXX. EASTES continued to discuss the Signal messaging app, stating that it was encrypted and was “the originator of probably the best E2E protocol around...”. The UCA downloaded the Signal messaging application, created an account, and sent his Signal username to EASTES, who replied that Signal “uses phone numbers for lookups lol, one sec”.

22. On the Signal encrypted messaging app, EASTES’ account appeared as “Kisuke” with the same phone number as the one EASTES had texted from. EASTES opened the message string with “Hello again” at approximately 2304 hours. EASTES defined “E2E” as encryption and asked the UCA “what kind of taboos you into”. The UCA responded “Well, young” and “You?” to which EASTES replied “<3” (heart) and “Same”. EASTES continued “Like I said, ‘need something smooth to wrap my meat around’”. When asked, EASTES said he had no nieces or nephews in state, but the ones out of state were “9 and under.” EASTES asked “WBU” (what about you?) and the UCA responded, “yea, got some around”. EASTES replied directly to this message with “Bred I hope XD [big smiley face]”.³

2 Punctuation is placed outside of quotation marks to accurately reflect the messages, and chat reactions are omitted. Emoticons (emojis) are described as applicable.

3 The term “bred,” or “to breed,” in some groups, refers to unprotected sexual intercourse, and

23. The UCA told EASTES that he has step-kids, to which EASTES replied “Ahh, nothing wrong with that. Best that someone steps up to daddy them”. The UCA responded “Sometimes you got to, am I right?” to which EASTES said “If I had a chance lol”. When asked if EASTES had any recent experience, he said, “Not since I was a preteen, sadly” and “Unless you count licking my nephew, and looking while changing his little brother”. EASTES clarified that he meant just kissing his nephew’s neck when putting him to bed. EASTES asked “Don’t get to play with your stepkids I take it/” and asked how old they were. The UCA responded that they are “7 n 9”, and EASTES said “Fuck I wish I could cuddle” and then “Be fun to breed them too, but how likely is that [laughing/crying smiley face]”. EASTES then sent three images of Child Sexual Abuse Material in Signal.

more specifically in some groups, unprotected anal intercourse.



B. EASTES Distributes Three Images of Child Sexual Abuse Material

24. The first image appears to depict a male infant or toddler, approximately between six-months and twenty-four months in age, lying on his back on a lime green cushion. The infant/toddler's fleece pajamas are unzipped, and his unfastened diaper lies under him. The infant/toddler's anus and genitals face the camera while an adult hand holds infant/toddler's feet up. Six L-shaped metal rods are attached to a large circular metal ring with thumb screws, inserted into and spreading the anus of the infant/toddler to an obviously excruciatingly painful

extent, markedly larger in circumference than that of the adult's thumb, and visually exposing the infant/toddler's rectum to the camera.

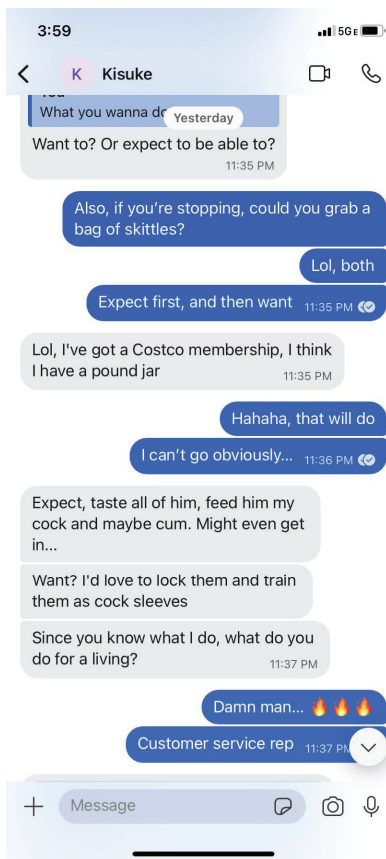
25. The second image appears to depict a male child, approximately two to three years of age, wearing a blue and gray V-neck shirt. The face of the child is shown with what appears to be semen in and around the mouth of the child and dripping out of the child's mouth.

26. The third image appears to depict a male child, approximately five to seven-years-old with only a fluorescent yellow shirt on in front of a purple and pink background. The child faces away from the camera and is bent forward at the waist, using his hands to spread his buttocks so the child's rectum is visible. The child's anus and genitals are visible to the camera and an approximately quarter-sized red mark or bruise is visible on his right buttock.

C. EASTES Continues Conversation and Plans to Purchase Candy and Sex Abuse Devices

27. The UCA stated that a neighbor had "helped him out" a little, to which EASTES said "I'd love to help too if I could". The UCA stated he had been "warming up my 7" and "The 7 likes to be naked and stuff and secret" to which EASTES directly replied "He's almost begging for it lol." EASTES discussed his own penis size. The UCA asked "What do you think would be good to try?" EASTES replied "Toys. Beads especially." and "Probably a plug too". The UCA stated that he didn't have those, and EASTES replied "I can pick a set up in the morning. No problem" and "Or RN". The UCA stated the child's mother would be back from a trip tomorrow but tonight would work, and EASTES asked "Ahh, Should I pick some up and come over?" and "Maybe bring my porn stash..." The UCA replied "I'm down to share. I do t have a lot" and EASTES replied directly "You have something more valuable tho. A willing boy :p". When the UCA said there couldn't be any marks, EASTES said "Of course, they gotta like it."

28. The UCA asked EASTES what he wanted to do, and EASTES said “Want to?” Or expect to be able to?” The UCA asked for both, and EASTES said “Expect, taste all of him, feed him my cock, and maybe cum. Might even get in...” and “Want? I’d love to lock them and train them as cock sleeves”. EASTES agreed to bring skittles per the UCA’s request and asked what kind of work the UCA does. EASTES then replied directly to his previous message and said, “And turn them into greedy piss drinkers”. EASTES asked “Should I grab lube too?” and said he would get silicone and water lubricant, asked for an address, and asked for pics of them. When asked, EASTES said he would not be driving his semi and would be in a car. The UCA provided a general location to meet and EASTES asked where he should park. EASTES again asked “No pics from you then?” to which the UCA sent a photo of his jacket and face.



29. At approximately 0005 hours, EASTES replied that he was almost on the way, and was toy shopping (for sex abuse devices). The UCA provided the predetermined meeting address in West Valley City, UT and asked if EASTES drank beer. EASTES replied that he was more of a liquor guy, “but I don’t want anything between him and my tongue”. EASTES then said, “Couldn’t find the beads I wanted, but got something fairly close, and got a plug too”. At approximately 0015 hours, EASTES said he was 10 minutes out and was not sure where to park. The UCA sent a map pin for the predetermined meeting location and a second one of where to park. The UCA said he was giving his fictitious child some ice cream and provided a fictitious name of the child. EASTES said he had almost forgotten the skittles candy. At approximately 0033 hours, EASTES updated that he was “5 min”.

D. EASTES Arrives and is Arrested with Skittles, Sex Abuse Devices, SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE

30. At approximately 0040 hours, a red Chevrolet Aveo bearing Utah plate Y099AR drove past the first entrance to the apartment complex and pulled into the second entrance of the predetermined meeting location as if unfamiliar with the area. Agents in the south end of the parking area confirmed that the vehicle was occupied by one person, a male, and then confirmed that he was the same person as the profile picture from EASTES’s Application A profile picture. EASTES attempted twice to back into the parking spot the UCA had sent by cellphone map-pin. Once backed into the parking area, EASTES asked “which unit am I headed to?” The UCA replied with a fictitious unit number while agents watched from a neighboring vehicle, and EASTES exited the car.

31. Agents and officers approached EASTES in several vehicles, all with police lights activated, exited the vehicles, and issued loud and clear verbal commands. EASTES

nervously dropped his cellphone on the driver's seat of the car and a purple package of skittles on the ground next to the driver's door of the car. EASTES complied with police direction and walked backward to agents where he was arrested and patted down. On EASTES' person, in a pocket, agents located a micro-SD card in a USB adapter attached to a short, red USB-C cable that would interface with the SUBJECT CELLPHONE.

32. EASTES' Utah Commercial Driver License in his wallet identified him as Kendrick Aristotle EASTES (DOB 06/14/1991) with physical descriptors of a 6'00", 220 lb. male with brown hair and green eyes, matching his physical description posted on Application A. EASTES' image and Driver License photo also matched his user photo on Application A.

33. On the driver's seat of the red Chevrolet was EASTES' cellphone, a plastic bag containing Gossip Hearts n' Studs pink anal beads, an orange Rooster anal device, a JET The Plug anal plug, JO XTRA SILKY personal lubricant, Slippery Stuff Personal Liquid Lubricant, BUTT EZE desensitizer, a receipt from Doctor John's for these items, and two Walmart receipts. The items were all in original packaging. The Doctor John's receipt was dated 02-17-2023 at 0009 hours for a total of \$122.20. Each of these items was collected and preserved as evidence.

34. Upon interview, EASTES exercised his 5th Amendment right and elected not to speak with agents.

35. As set forth above, EASTES initiated a conversation on Application A with the UCA. In the conversation, EASTES expressed his desire and then his intention to sexually abuse and sodomize a seven-year-old child. EASTES distributed three images of apparent CSAM to the UCA. EASTES communicated that he would bring his "porn stash," sexual lubricant, sex abuse devices to use on the child, and candy for the child. EASTES drove to the location of the child, and upon contact with agents and his arrest, had with him the SUBJECT CELLPHONE,

and SUBJECT STORAGE DEVICE with USB adapter that would interface with the SUBJECT CELLPHONE. The SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE were seized and booked in as evidence.

36. I know that Application A is accessed via a smart phone. I also know that people often carry cellular telephones such as smartphones on their persons and/or in their vehicles, and external storage devices can be connected to such cellular telephones for additional storage. EASTES distributed apparent CSAM, stated he was bringing his (child) pornography collection, and arrived with electronic storage devices capable of storing CSAM. There is probable cause to believe that much of this evidence is digital in nature; based on my training and experience and the information set forth above, including the Background on Internet and CSAM (Child Pornography), there is probable cause to believe that such evidence as outlined in **Attachment B** will be found on the SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE described in **Attachment A**.

Search and Seizure of Digital Data

37. This application seeks permission to search for and seize evidence of the Target Crimes described above, including evidence of how computers, digital devices, and digital storage media were used, the purpose of their use, and who used them.

38. Based on my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that data in digital form can be stored on a variety of systems and storage devices, including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items.

39. I know from my training and experience, as well as from information found in publicly available materials, that these digital devices offer their users the ability to unlock the device via the use of a fingerprint, thumbprint, or facial recognition in lieu of a numeric or alphanumeric passcode or password. These features are commonly referred to as biometric authentication and their availability is dependent on the model of the device as well as the operating system on the device. If a user enables biometric authentication on a digital device, he or she can register fingerprints, or his or her face, to unlock that device.

40. In some circumstances, biometric authentication cannot be used to unlock a device, and a passcode or password must be used instead. These circumstances include: (1) the device has been turned off or restarted; (2) the device has received a remote lock command; (3) too many unsuccessful attempts to unlock the device via biometric authentication are made; (4) too many hours have passed since the last time the device was unlocked; and (5) the device has not been unlocked via biometric authentication for a period of time and the passcode or password has not been entered for a certain amount of time. Thus, when law enforcement encounters a locked digital device, the opportunity to unlock the device via biometric authentication exists only for a short time.

41. The passcode or password that would unlock the SUBJECT CELLPHONE is not known to law enforcement. Thus, it is necessary to press the fingers of EASTES to the SUBJECT CELLPHONE's sensor, or hold the phone up to EASTES' face, in an attempt to unlock the devices for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device via biometric authentication is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant. I therefore request that the Court

authorize law enforcement officers to press the fingers, including thumbs, of EASTES to the fingerprint sensor of the SUBJECT CELLPHONE, or to hold the device equipped with facial recognition authentication up to EASTES' face, to unlock the device and thereby allow investigators to search the contents as authorized by this warrant.

Forensic Imaging of Data Storage Devices

42. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant. I also know that during a search of premises it is not always possible to create a forensic image of or search digital devices or media for data for various reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. Because there are so many different types of digital devices and software in use today, it is difficult to anticipate all the necessary technical manuals, specialized equipment, and specific expertise necessary to conduct a thorough search of the media to ensure that the data will be preserved and evaluated in a useful manner.

b. Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data not readily apparent to the casual user. The recovery of such data may require the use of special software and procedures, such as those used in a law enforcement laboratory.

c. The volume of data stored on many digital devices is typically so large that it is generally highly impractical to search for data during the execution of a physical search of premises. Storage devices capable of storing 500 gigabytes to several terabytes of data are

now commonplace in desktop computers. It can take several hours, or even days, to image a single hard drive; the larger the drive, the longer it takes. Depending upon the number and size of the devices, the length of time that agents must remain onsite to image and examine digital devices can make doing an on-site search impractical.

Laboratory Setting May Be Essential for Complete and Accurate Analysis of Data

43. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, may be essential to conduct a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

44. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created,

modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

45. *Latent Data:* Searching digital devices can require the use of precise scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's operating system may keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

46. *Contextual Data:*

a. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and

the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious

software, evidence of remote control by another computer system, or other programs or software, may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

Search of SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE

47. As described above and in **Attachment B**, this application seeks permission to search the SUBJECT CELLPHONE and the SUBJECT STORAGE DEVICE for CSAM in whatever form they are found. The warrant applied for would authorize the seizure of electronically stored information or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

48. As further described in **Attachment B**, this application seeks permission to locate not only digital files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the SUBJECT CELLPHONE and the SUBJECT STORAGE DEVICE were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be in the SUBJECT CELLPHONE and the SUBJECT

STORAGE DEVICE.

49. Law enforcement personnel will examine the SUBJECT CELLPHONE and the SUBJECT STORAGE DEVICE to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in **Attachment B**. To the extent law enforcement personnel discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

50. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a “hash value” library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

Retention of Image

51. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Request for Sealing

52. I further request that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrants, including the application, this affidavit, the attachments, and the requested search warrants. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing

investigation in which not all targets have been identified. Disclosure of the information in this affidavit at this time may cause flight from prosecution, the destruction of or tampering with evidence, or could otherwise seriously jeopardize the integrity of the ongoing investigation.

Conclusion

53. Based on the foregoing, I have probable cause to believe that Kendrick Aristotle EASTES committed the SUBJECT OFFENSES and that contraband and evidence, fruits, and instrumentalities of those violations, as described in **Attachment B**, will be located in the SUBJECT CELLPHONE and the SUBJECT STORAGE DEVICE as described in **Attachment A**.

JEFFREY M
CHMIELEWSKI

Digitally signed by JEFFREY M
CHMIELEWSKI
Date: 2023.03.01 13:41:43 -07'00'

JEFFREY M. CHMIELEWSKI
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this __1st__ day of March, 2023.

Daphne A. Oberg

DAPHNE A. OBERG
United States Magistrate Judge

Approved:

MARK
HIRATA

Digitally signed by
MARK HIRATA
Date: 2023.03.01
13:05:55 -07'00'

MARK Y. HIRATA
Assistant United States Attorney

ATTACHMENT A
PROPERTY TO BE SEARCHED

1. The SUBJECT CELLPHONE is described as a Google Pixel Cellphone, gray in color, in a two-tone pink and maroon case. The SUBJECT CELLPHONE is in a locked state, and device serial number and the International Mobile Equipment Identity (IMEI) are unable to be read without accessing the SUBJECT CELLPHONE.



2. The SUBJECT STORAGE DEVICE is a SanDisk Extreme Plus Micro SD Card 128 GB with USB-A microSD car reader and a red JSAUX USB-A to USB-C cable and adapter.



ATTACHMENT B

LIST OF ITEMS AND INFORMATION TO BE SEIZED AND SEARCHED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of Coercion and Enticement in violation of 18 U.S.C. § 2422(b), Distribution of Child Pornography in violation of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), and Possession of or Accessing with Intent to View Child Pornography in violation of 18 U.S.C. §§ 2252(a)(4) and 2252A(a)(5)(B), and are contained in the SUBJECT CELLPHONE or SUBJECT STORAGE DEVICE as described in

Attachment A:

1. All CSAM, including:
 - a. Child pornography, as defined in 18 U.S.C. § 2256(8),
 - b. Visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
 - c. Child erotica;
 - d. Records, information, and items relating to a sexual interest in children;
2. Evidence of who used, owned, or controlled the SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

3. Evidence of the presence or absence of software that would allow others to control the SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - a. Evidence of the lack of such malicious software;
 - b. Evidence indicating how and when the SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE were accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE user;
 - c. Evidence indicating the SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE user's knowledge and/or intent as it relates to the crime(s) under investigation;
 - d. Evidence of the attachment to the SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE of other storage devices or similar containers for electronic evidence;
 - e. Evidence of programs (and associated data) that are designed to eliminate data from the SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE;
 - f. Evidence of the times the SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE was used;

- g. Records of or information about Internet Protocol addresses accessed by the SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE;
- h. Records of or information about the SUBJECT CELLPHONE and SUBJECT STORAGE DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- i. Contextual information necessary to understand the evidence described in this attachment;
- j. Records and information tending to identify or locate any children depicted in child pornography or suspected of being sexually exploited in any way;
- k. Records and information relating to the sexual exploitation of children, including correspondence and communications between messaging platform users;
- l. Records and information showing access to and/or use of Messaging Platform A;
- m. Records, information, and items relating to Messaging Platform A; and
- n. Records and information relating or pertaining to the identity of the person or persons using or associated with Application A user Kisuke, the telephone account associated with phone number 505-333-XXXX, and the Signal user account associated with Kisuke and with phone number 505-333-XXXX.

During the execution of the search of the SUBJECT CELLPHONE described in **Attachment A**, law enforcement personnel are also specifically authorized to compel EASTES

to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of the SUBJECT CELLPHONE.

This warrant does not authorize law enforcement personnel to compel from EASTES the password or any other means that may be used to unlock or access the SUBJECT CELLPHONE, as described in the preceding paragraph.